

Digital Video Broadcasting (DVB) CBMS Service Purchase and Protection Open Framework System Architecture Specification

European Broadcasting Union



Union Européenne de Radio-Télévision

THIS IS A PROVISIONAL DVB DOCUMENT. IT MAY BE CHANGED BEFORE FINAL ADOPTION BY DVB. THIS PROVISIONAL DOCUMENT IS FOR DISCUSSION PURPOSES ONLY. IMPLEMENTERS ARE NOT ENTITLED TO RELY ON THIS PROVISIONAL DOCUMENT. WHERE POSSIBLE, ITEMS FOR WHICH CONSENSUS HAS NOT BEEN REACHED ARE SUITABLY MARKED, FOR EXAMPLE BY SQUARE BRACKETS. IMPLEMENTERS SHOULD ALSO NOTE THAT ONLY FINAL SPECIFICATIONS ADOPTED BY DVB ARE (SUBJECT TO THE "NEGATIVE DISCLOSURE" RIGHTS OF MEMBERS) ENTITLED TO THE IPR LICENSING TERMS OF DVB'S MEMORANDUM OF UNDERSTANDING.



Reference

REN/JTC-DVB-102

Keyword

broadcasting, digital, DVB, MPEG, service, TV,
video

ETSI

650 Route de Luciole
F-06921 Sophia Antipoli Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:

<http://www.etsi.org>

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in content between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printer of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at <http://www.etsi.org/tb/status/>

If you find errors in the present document, send your comment to:
editor@etsi.fr

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restrictions extend to reproduction in all media.

© European Telecommunication Standard Institute 2000.
© European Broadcasting Union 2000.
All rights reserved.

Content

Intellectual Property Right	5
Foreword	5
1 Scope	6
2 Reference	6
3 Definition and abbreviation	6
3.1 Definition	6
3.2 Abbreviation	7
4 Introduction	8
5 DVB-CBMS System Architecture	8
5.1 Overview	8
5.2 Content & Service Protection Architecture	9
5.2.1 Key Management System (KMS)	9
5.2.1.1 Registration	9
5.2.1.2 Authorization and Right Issuing	10
5.2.1.3 Service Protection	10
5.2.1.4 Copy Protection	10
5.2.2 Key Management System Device Agent (KDA)	10
5.2.3 Scrambler	10
5.2.4 Descrambler	10
5.2.5 Session Setup	10
6 Security Mechanism	11
6.1 Entitlement Management Message (EMM) Stream	11
6.1.1 EMM Stream Transport and Signalling	11
6.1.1.1 Target_CA_system_decryptor	12
6.2 Entitlement Control Message (ECM) Stream	12
6.2.1 ECM Stream Transport and Signalling	13
6.2.2 ECM Stream Binding	14
7 Roaming	15
7.1 Roaming Overview	15
7.2 Security Architecture	16
7.2.1 Registration	16
7.2.2 Authorization	17
7.2.3 Right Issuing	17
7.2.4 Service Protection	17
7.2.5 Content Protection	17
7.3 Key Management and Distribution	17
7.3.1 Daily Encryption Key	17
7.3.2 Service Encryption Key	18
7.3.3 Traffic Encryption Key	18
7.4 Key Generation and Validation at the Device	18
7.5 Roaming Message	18
7.5.1 Device Roaming Request	18
7.5.2 Roaming Request	19
7.5.3 Roaming Request Response	19
7.5.4 Roaming_Initial_EMM	20
7.5.5 Roaming_Service_EMM	21
7.5.6 Roaming_Service_ECM	22
8 Annex A (Informative): Adaptation of DVB Simulcrypt interface to the DVB-H Environment	22
8.1 Reference DVB-Headend Architecture	22
8.2 DVB-H Headend Architecture and Interface	23
8.3 DVB-H Headend Architecture for Roaming Support	24

8.3.1	Roaming ECM	25
8.3.2	Roaming EMM	25
9	Annex B (Informative): Using OMA BCAST as a Key Management System	26
9.1	Overview	26
9.2	Registration	26
9.3	EMM	26
9.4	ECM	26
	Bibliography	27
10	History	28

Intellectual Property Right

IPR essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to the essential IPR, if any, is publicly available for **ETSI member and non-member**, and can be found in ETSI SR 000 314: *"Intellectual Property Right (IPR); Essential, or potentially Essential, IPR notified to ETSI in respect of ETSI standard"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (<http://www.etsi.org/ipr>).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPR not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This European Standard (Telecommunication series) has been produced by the Joint Technical Committee (JTC) Broadband of the European Broadcasting Union (EBU), Comité Européen de Normalisation ELECTrotechnique (CENELEC) and the European Telecommunication Standard Institute (ETSI).

NOTE: The EBU/ETSI JTC Broadband was established in 1990 to co-ordinate the drafting of standards in the specific field of broadcasting and related fields. Since 1995 the JTC Broadband became a tripartite body by including in the Memorandum of Understanding also CENELEC, which is responsible for the standardization of radio and television receivers. The EBU is a professional association of broadcasting organizations whose work includes the co-ordination of its members' activities in the technical, legal, programme-making and programme-exchange domains. The EBU has active members in about 60 countries in the European broadcasting area; its headquarters are in Geneva.

European Broadcasting Union
CH-1218 GRAND SAconnex (Geneva)
Switzerland
Tel: +41 22 717 21 11
Fax: +41 22 717 24 81

Founded in September 1993, the DVB Project is a market-led consortium of public and private sector organizations in the television industry. Its aim is to establish the framework for the introduction of MPEG-2 based digital television services. Now comprising over 200 organizations from more than 25 countries around the world, DVB fosters market-led systems, which meet the real needs, and economic circumstances, of the consumer electronics and the broadcasting industry.

National transition date
<p>Date of adoption of this EN:</p> <p>Date of latest announcement of this EN (doa):</p> <p>Date of latest publication of new National Standard or endorsement of this EN (dop/e):</p> <p>Date of withdrawal of any conflicting National Standard (dow):</p>

1 Scope

This specification addresses the area of 'Service Purchase and Protection' for DVB-CBMS System. The present document specifies the common mandatory elements used for service protection in DVB-CBMS system:

1. Scrambling Technology based on ISMACryp 1.0
2. Security mechanism for IP Datacast over DVB-H, to allow the insertion and carriage of ECM and EMM for different Key Management System.
3. An architecture that permits global roaming.
4. Headend architecture based on DVB Simulcrypt

This specification should be read in conjunction with:

- ETSI EN xxx xx2 DVB CBMS Service Purchase and Protection Open Framework, Content Encryption Specification.
- ETSI EN xxx xx3 DVB CBMS Mobile Device Security Framework.

2 Reference

- [1] ETSI TS 103 197 DVB SimulCrypt; Head-end architecture and synchronization - v1.3.1 (03/01)
- [2] RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practice Framework
- [3] RFC 3447, Public-Key Cryptography Standard (PKCS) #1: RSA Cryptography Specification Version 2.1
- [4] RFC 3174, US Secure Hash Algorithm 1 (SHA1)
- [5] Internet Streaming Media Alliance Encryption and Authentication Specification, Version 1.0, February 2004, Internet Streaming Media Alliance.
- [6] ETR 162 Digital broadcasting system for television, sound and data service; Allocation of Service Information (SI) code for Digital Video Broadcasting (DVB) system
- [7] ETSI EN xxx xx2 DVB CBMS Service Purchase and Protection Open Framework, Content Encryption Specification.
- [8] ETSI EN xxx xx3 DVB CBMS Mobile Device Security Framework.

3 Definition and abbreviation

3.1 Definition

For the purpose of the present document, the following terms and definitions apply:

ISMACryp: Define an end-to-end content encryption system for media carried over RTP stream and ISO based media file.

Media Access Unit: A Media Access Unit (AU) is the smallest data entity to which timing information can be attributed. In the case of audio an AU is an audio frame and in case of video a picture.

Interaction Channel: A bi-directional channel established between the IPDC Service Network and the IPDC mobile terminal for connectivity/interaction purpose.

Roaming: End-user accessing IPDC service in another (foreign) network (in this case either DVB-H or cellular) than the home network. Service roaming means that the same IPDC service of the home network can be accessed in a foreign network. User roaming means that a user has access to the IPDC service of a foreign network.

Device: mobile terminal that is capable of receiving IP Datacast transmission over DVB-H network. The terminal may be capable of interacting with service provision subsystem and commerce subsystem through a cellular network. The mobile terminal may include an optional embedded Secure Hardware, such as a SIM card.

OMA BCAST: is a fully standardized system allowing operator to control access and usage of broadcast content on mobile device. The full specification are currently being drafted within OMA.

3.2 Abbreviation

For the purpose of the present document, the following abbreviation apply:

AC	Access Criteria
ACG	Access Criteria Generator
CA	Conditional Access
CAS	Conditional Access System
CAS_ID	CA System ID
CTR	Counter
DVB	Digital Video Broadcasting
MPEG	Moving Picture Expert Group
DEK	Daily Encryption Key
DVB	Digital Video Broadcasting
DVB-H	DVB-Handheld
DVB-T	DVB-Terrestrial
ECM	Entitlement Control Message
ECMG	ECM Generator
EIS	Event Information System
EMM	Entitlement Management Message
EMMG	EMM Generator
HO	Home Operator
IP	Internet Protocol
IPDC	IP DataCast
ISMA	Internet Streaming Media Alliance
ISO	International Standard Organization
KDA	Key Management System Device Agent
KMS	Key Management System
KSM	Key Stream Message
MPEG	Moving Picture Expert Group
PSS	Probabilistic Signature Scheme
RO	Right Object
RSA	Rivest, Shamir and Adelman
RTP	Real-time Transport Protocol
SC	Smart Card
SCS	Simulcrypt Synchroniser
SDP	Session Description Protocol
SEK	Service Encryption Key
SHA	Standard Hash Algorithm
SIM	Subscriber Identity Module
SRTT	Secure Real-Time Transport Protocol
TEK	Traffic Encryption Key
Uim bf	Unsigned integer, most significant bit first
URL	Uniform Resource Locator
USIM	Universal Subscriber Identity Module
VO	Visiting Operator

4 Introduction

This document provides a description of a service protection architecture for DVB-CBMS system, specifies which part of this system are standardized and provide specification for the part or refer to other document providing such specification.

The basic concept governing this specification is the Open Framework approach, whereby a number of basic building blocks are standardized to provide interoperability, and additional non-standardized blocks may be used where required for added value and hooked into the system using a number of standard interoperability points.

The service protection framework follows the DVB1.0 solution providing protection against security attacks using just-in-time key distribution and regular key refreshing. The specification facilitates horizontal deployment of devices, allows for roaming and enables variegated key management system in response to market need.

This document specifies signalling and delivery mechanisms for authorization, rights and key management stream used by Key Management System. It includes a scheme for global roaming and defines a headend reference architecture based on DVB Simulcrypt. Content protection is based on the ISMACryp 1.0 content scrambling standard, predicated on the AES cipher.

5 DVB-CBMS System Architecture

5.1 Overview

Figure 1 below shows the overall high-level view of the end-to-end system.

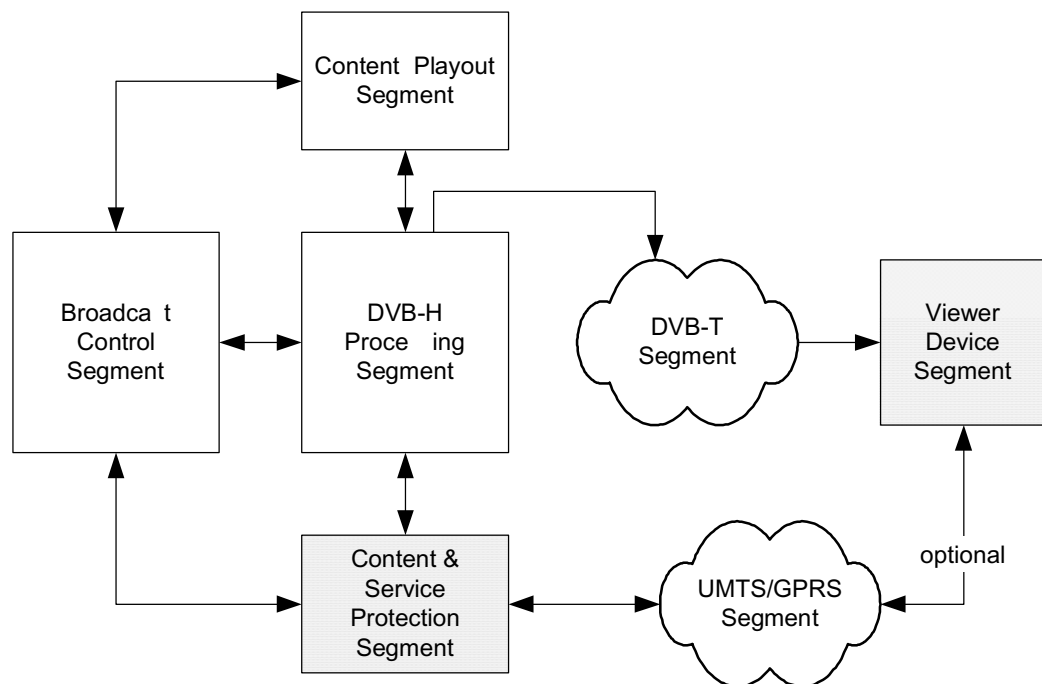


Figure 1: Overview of DVB-CBMS Architecture

In this high level view the following segments are presented:

Segment	Function
Broadcast Control Segment	Control what content is being played at a given time, and using what access criteria
Content Playout Segment	Responsible for the encoding, storage, and playout of content.

Segment	Function
DVB-H Processing Segment	Responsible for: <ol style="list-style-type: none"> 1. Creation of the DVB-H stream, including combining any data presented by the Content and Service Protection Segment 2. Presenting this data to the DVB-T Segment for transmission.
Content & Service Protection Segment	Responsible for: <ol style="list-style-type: none"> 1. Scrambling content 2. Maintaining container used to carry entitlement and access right 3. (Optional) Communication with the viewer device on a return channel, if such a back channel exists
Viewer Device Segment	This segment consists of the viewer device and optional embedded SIM card. Receives the DVB-T signal, parses the DVB-H stream, and is responsible for descrambling and rendering.

This document concentrates on the Viewer Device Segment and the Content & Service Protection Segment.

5.2 Content & Service Protection Architecture

An overview of the Content and Service Protection architecture is depicted in Figure 2: -

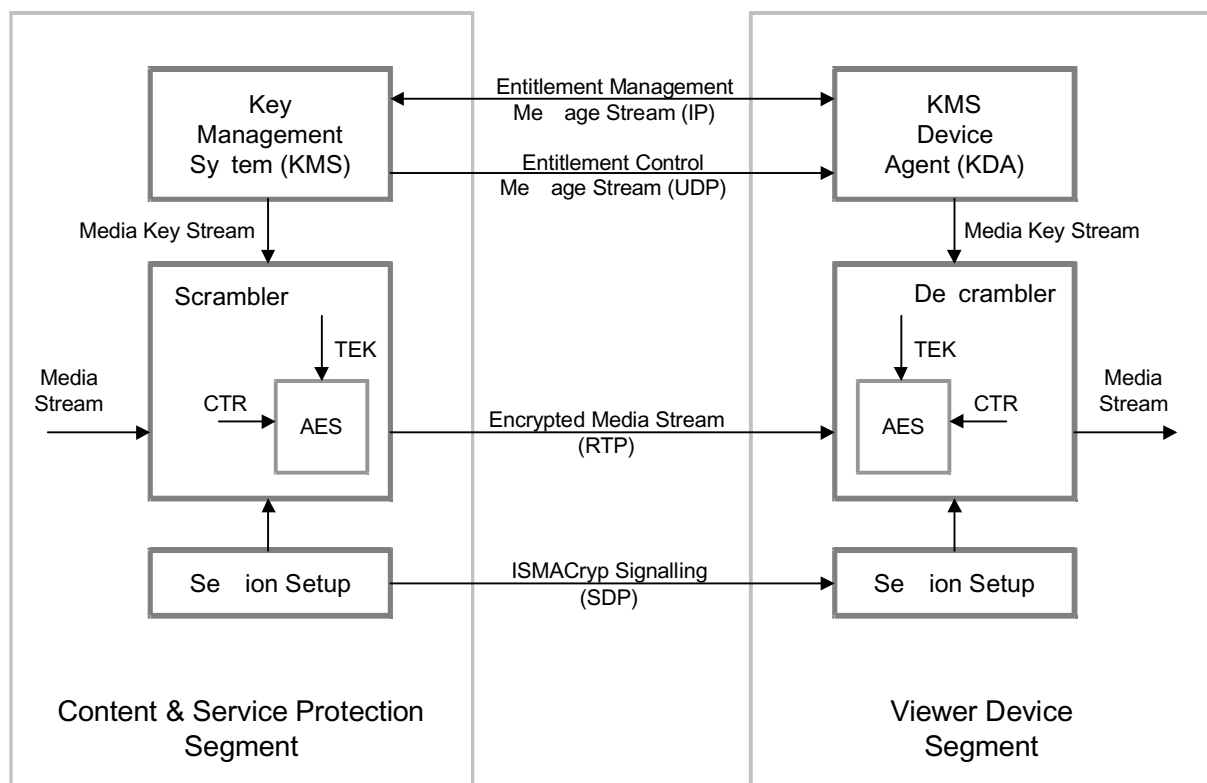


Figure 2: Overview of Content and Service Protection Architecture

5.2.1 Key Management System (KMS)

The Key Management System supports the following security function: -

5.2.1.1 Registration

Device registration shall take advantage of the interaction channel, when available. The use of the interaction channel for device registration shall be Key Management System (KMS) specific.

5.2.1.2 Authorisation and Right Licensing

Device authorisation and service access right shall be delivered to the device using the Entitlement Management Message (EMM). This specification defines the signalling and transport mechanism for the EMM stream. The content and format of the EMM are KMS specific.

The KMS may utilize either the broadcast channel or interaction channel for delivering EMM to the device.

5.2.1.3 Service Protection

Traffic Encryption Key (TEK) are applied directly to the scrambler to protect the content. The TEK are sent to the device in Entitlement Control Message (ECM). This specification defines the signalling, binding and transport mechanism for the ECM stream. Additionally, the method of synchronisation of the ECM stream with the encrypted media stream are defined. The content and format of the ECM are KMS specific.

The ECM are delivered over the broadcast channel with the encrypted media stream. The messages are cycled to support random access to broadcast service.

5.2.1.4 Copy Protection

In case content needs to be securely exported to a separate post-delivery copy-protection system such as DVB-CPCM, the Usage State Information needed by such a system can be carried by the Key Management System.

5.2.2 Key Management System Device Agent (KDA)

The Key Management System Device Agent (KDA) contains vendor-specific logic required to control the descrambling process for a specific Key Management System.

The KDA performs the following security function :-

1. Reception of EMM from the KMS by means of the broadcast or interactive network.
2. Secure generation of device authorisation from the received EMM.
3. Reception of the ECM stream for the selected service from the broadcast network.
4. Secure generation of the Media Key Stream (TEK) from the received ECM stream.
5. Applying the Media Key Stream to the descrambler, controlling the decryption of the Encrypted Media Stream.

5.2.3 Scrambler

The media stream is encrypted with the TEK using ISMACryp 1.0 AES-128 Counter Mode. The details of Content Encryption Scheme can be found in Reference [7].

5.2.4 Descrambler

The media stream is decrypted with the TEK using ISMACryp 1.0 AES-128 Counter Mode. The details of Content Decryption Scheme can be found in Reference [7].

5.2.5 Session Setup

The Session Information used by the KDA for controlling access to the Service Layer is carried in its own Session Layer using SDP.

6 Security Mechanism

The following mechanisms are supported by this specification: -

1. Entitlement Management Mechanism (EMM)
2. Entitlement Control Mechanism (ECM)

The mechanisms are utilized by Key Management System to secure access to the encrypted media stream. This specification defines a scheme for identifying and delivering the mechanisms within the IPDC transmission. The mechanisms are specified as an extension to the existing ISMACryp 1.0 specification.

The security mechanisms supported by this specification include regular key refreshing and just-in-time key distribution. Together, the mechanisms shall protect real-time broadcast content against any key distribution and security attack.

Figure 3 below shows the reception relationship between the EMM and ECM mechanisms.

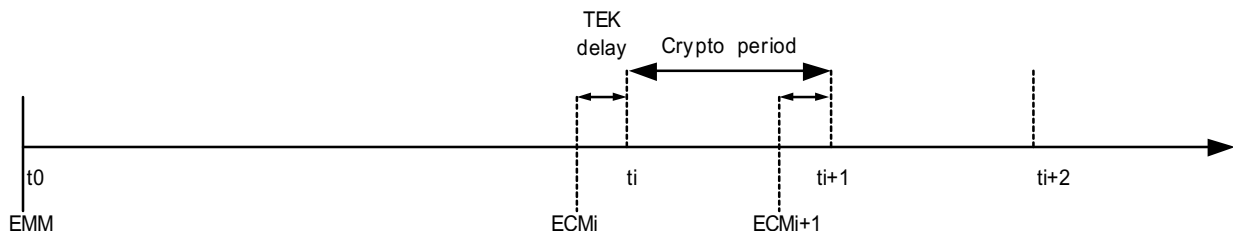


Figure 3: EMM/ECM timing

The scrambling mechanism supports the concept of crypto-period, allowing a time-varying sequence of TEK to be applied to the scrambler. The encrypted media stream and the ECM stream contain the necessary information to allow synchronization of the encryption and decryption process. The authorization and service access right are delivered to the device ahead of consumption time using the EMM stream.

6.1 Entitlement Management Mechanism (EMM) Stream

EMM are generated by the KMS to dynamically associate profile to the end user in a secure manner. EMM convey the necessary authorization/right for the reception of broadcast media content for a single end user or group of end user. EMM encompass the different business rule that allow broadcaster to implement multiple business model, such as subscription, pay-per-view, pay-per-time, etc. In addition, EMM may provide the security mechanism for initiating control action on a device, for example to control software download.

EMM can be broadcast using the DVB-H network or retrieved from a URL using the interactivity channel (other delivery method for EMM are not precluded by this specification, e.g. SMS). In the case of broadcast, the mechanisms may be sent on an operator configured channel, so as to optimize delivery of the mechanisms stream to device. During the process of receiving the EMM, the device will typically be authenticated, authorized, and accounted to the requested content or service.

6.1.1 EMM Stream Transport and Signalling

The EMM are transported in stream of IP/UDP packet addressed to the IP address signalled in the DVB IP Notification Table (INT) as described below. Each IP packet contains any number of complete EMM. No header or other form of signalling is required in the packet, only the EMM themselves.

DVB has defined the IP Notification Table to provide a flexible mechanism for carrying information about the location of IP/MAC stream within DVB network. Through the use of a flexible syntax, extensive targeting and notification descriptor mechanism, the table can be easily extended to cover additional requirements in the DVB IP/MAC domain and especially for IPDC over DVB-H. The full specification is available in the DVB specification EN 301192 published by ETSI.

For IPDC over DVB-H, the proposition is to allocate one or more IP addresses to be listened to for each KMS provider. The INT table will provide the link between the IP address and the corresponding Transport Stream Packet Identifier

(PID) to filter on. On the e pecific PID , the EMM will be carried a regular IPDC over DVB-H ervice , meaning time- liced for power con umption efficiency.

The pecification allow for power efficiency, enabling a device to filter on a particular time- liced EMM stream by extracting the relevant PID/IP addre for the pecific KMS.

6.1.1.1 Target_CA_ y tem_de criptor

This pecification define a new de criptor for a ociating a pecific KMS with a particular EMM stream. The pecification reuse the DVB defined CA_ y tem_id to identify a pecific KMS.

INT Location : **Loop of table**: platform, operational

Action_type: 0x01

This de criptor target the group of receiver related to this KMS, and a ociated with the IP/MAC_ stream_location_de criptor it allow a device to locate the KMS pecific EMM stream, particular to the device KDA.

Name	No. of bit	Identifier
Target_CA_ y tem_de criptor() {		
de criptor_tag	8	uim bf
de criptor_length	8	uim bf
CA_ y tem_id	16	uim bf
Operator_id	16	uim bf
}		

Semantic : -

CA_ y tem_id: This 16-bit field identify the KMS. Allocation of the value of this field are found in ETR 162 [6].

Operator_id: This 16-bit field identify an operator. Allocation of the value of this field is under the control of the KMS identified by CA_ y tem_id and allow differentiating between operator using the same KMS.

6.2 Entitlement Control Message (ECM) Stream

ECM are generated by the KMS to securely transmit the media key stream with the encrypted media stream. ECM message also include the access right definition associated with the protected media content. The ECM stream is processed by the KDA to retrieve the media key stream required by the descrambler to decrypt the encrypted media stream: -

$$\text{media_key}[i] = \text{Decrypt}(\text{ECM}[i], \text{EMM})$$

Where in general, the EMM could be a combination of the current user profile and other service purchase characteristics associated with the end user. Characteristics include type of subscription, or the program purchased in the past by the end user.

The ECM consists of an in-band stream transmitted in parallel with the media stream. Key Indicator (KI) are placed into the media stream as a reference to the correct ECM message within the ECM stream. The media stream and KI format are described in reference [7].

ECM should be sent in regular cycle in a low frequency transmission. Both cycle and frequency are defined by the headend and can be synchronized with the DVB-H time-licing to minimize the number of ECM per time-lice. This would allow the device to compensate for missing ECM packet, while providing fast zapping between program. It is assumed that the ECM retransmission shouldn't increase the total media stream bandwidth by more than 1 percent.

Figure 4 below describes the headend subsystem required to encrypt the content and generate the ECM stream.

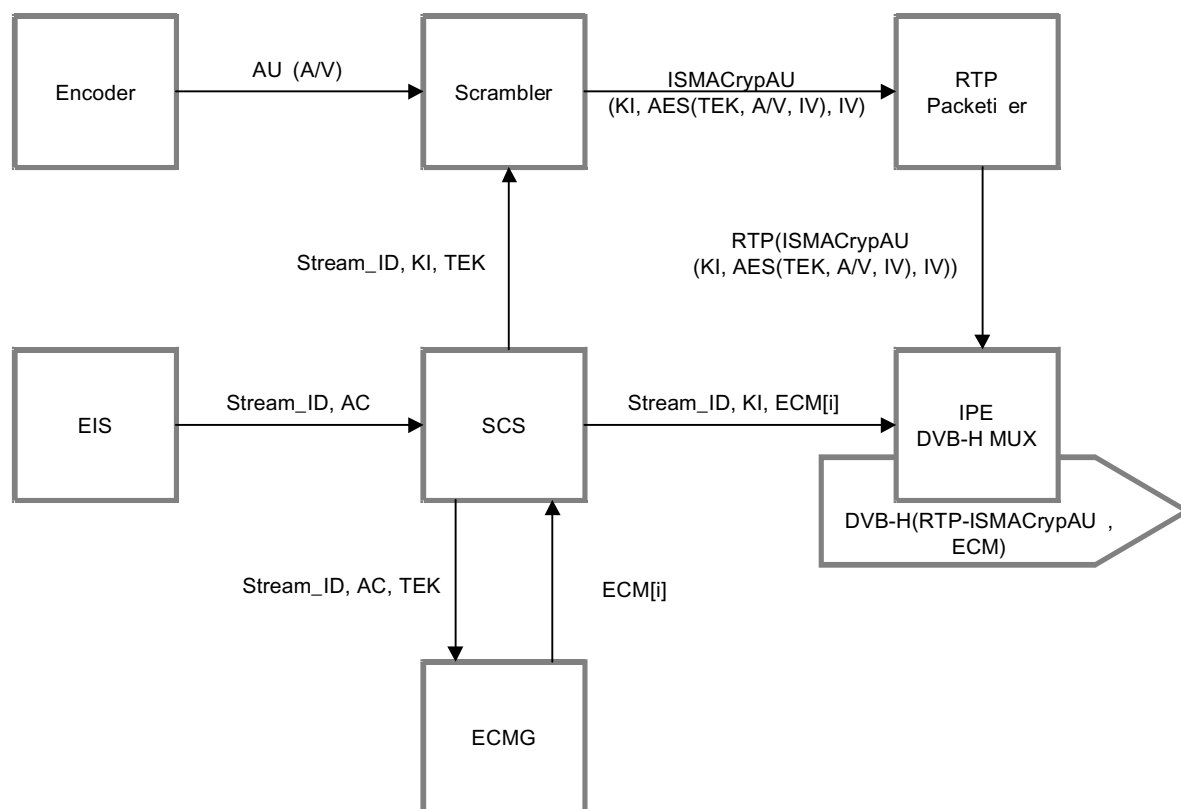


Figure 4: DVB-H Headend: Schematic Architecture

The ECM stream signalling support Simulcrypt, allowing multiple Key Management System to control a single protected media stream within the same broadcast network. The ECM transport mechanism provide flexible and optimized delivery for real-time broadcast application.

Each KMS is identified by the CAS identifier: CA_System_ID, as described in ETR 162 [6]. The identifiers are pre-defined providing a mapping between the ECM stream and the appropriate KMS.

6.2.1 ECM Stream Transport and Signalling

To support efficient ECM carriage, especially in the presence of Simulcrypt, each ECM stream is carried in its own UDP stream (a unique port is used for each ECM stream). A single UDP packet shall carry one or more complete ECM. In case several ECM are carried in a single UDP packet, they are placed one after the other in the packet without additional signalling.

SDP signalling (RFC 2327) is used to locate ECM stream.

SDP declaration of an ECM stream will have the following structure:

```

m=data 49230 UDP 99
a=rtpmap:99 dvbh-ecm/16000
a=fmtp:99 [PARAMS]
  
```

The table below describes the DVB-H-PARAMS field :

Descriptor	Type	Comment
DVBHStreamId	Integer	Stream identifier uniquely defined by the headend
DVBHCASId	Integer	KMS identifier
DVBHOperatorId	Integer	Operator identifier
DVBHAcce Right	String	Optional description or URL of the access right associated with the content

All parameters are mandatory, unless stated otherwise.

Example:

```
m=data 49230 UDP 99
a=rtpmap:99 dvbh-ecm/16000
a=fmtp:99 DVBHStreamId=10;
DVBHAcce Right =http://www.dvbhop.com/channel9.asp;
DVBHCASId=1559; DVBHOperatorId=1234;
```

6.2.2 ECM Stream Binding

The signalling described below allows the KDA to clearly identify which ECM stream is relevant for each media stream. Several media streams may reference the same ECM stream, thereby sharing the same TEK, but each media stream may also reference a different ECM stream.

A single media stream may reference several ECM streams, thereby supporting Simulcrypting, where different KMS provide secure delivery of the same TEK using their private ECM format.

Example: -

A service comprising a video stream and an audio stream, both encrypted with the same key, and protected by two different KMS will make use of 4 streams: one for the video, one for the audio, one for KMS#1 ECM stream and one for KMS#2 ECM stream.

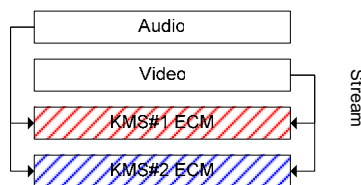


Figure 5: ECM Stream Binding

This way, the KDA will only listen to and process the ECM stream coming on the relevant port.

SDP signalling (RFC 2327) is used to describe the ECM stream(s) associated with each media stream.

The SDP media format will have the following structure (for an ISMACryp media stream):

```
m=video RTP/AVP 98
a=rtpmap:98 enc-generic-mp4
a=fmtp:98 [DVB-H-PARAMS] [other parameter]
```

The table below describe the DVB-H-PARMS field :

Descriptor	Type	Comment
DVBHECMStream	List of Integer triplet	List of CAS ID/Operator ID/ECM Stream ID triplet separated by a space. Each triplet take the form CASID/OperatorID/ECM Stream ID and indicate which ECM Stream ECM stream is relevant for that media stream, CAS ID and Operator ID. The Operator ID allow simulcrypting between multiple operator using the same KMS. The ECM Stream is identified by its DVBHStreamID parameter described above.

The [other parameter] field comprise all the other parameter required by the particular RTP payload, in particular those defined by ISMACryp.

Example:

m=video 0 rtp/avp 96

a=rtpmap:96 enc-generic-mp4/16000/1

a=fmtp:96 ISMACRYP_CRYPTOSUITE=AES_CTR_128; ISMACRYP_IV_LENGTH=4;
ISMACRYP_DELTA_IV_LENGTH=0; ISMACRYP_KEY_INDICATOR_LENGTH=1; ISMACRYP_SALT=base64,
AoIAE8BAQ8BAQOBSgABQKxkYXRhOmFwc;DVBHECMStream =1559/1234/10 101/34/11;

7 Roaming

7.1 Roaming Overview

Support of roaming between operator is an essential element of this proposal. Every device will have a KDA supporting the local operator service. Different KMS providers will offer support for the various business models in different markets.

However, there will be a baseline of service that all KMS will need to support for roaming. Every KDA will have to provide the function in the roaming architecture. It is possible that various operators will prefer to operate a baseline system that works only according to the roaming protocol.

In the following text, a service is the unit of sale: the operator selling the service defines it. Typical examples are: a TV channel for a day, a particular TV event, etc.

The players involved in the roaming scenario are the Home Operator, the Visiting Operator and the receiving device:

- The Home Operator (HO) is the operator that provides service in the Device's home network. The HO controls the KMS and KDA. If a SIM card is present in the device, the HO knows the secret contained therein.
- The Visiting Operator (VO) is the operator who provides service the device owner wants to consume. Content services are unlike voice or data transport services since the channel package offered in any two markets is likely to be quite different.

A VO has a roaming service relationship with the HO, at least as far as billing is concerned. That roaming relationship is out of the scope of this document.

A device has a HO-specified KDA. When the device owner roams to another market, there is a method in place by which they can choose service in the visited market. This can be automated if the device is two-way; or alternatively, it may require a phone call if the device does not have back channel capability.

7.2 Security Architecture

The roaming architecture support authentication, confidential key distribution and data protection for roaming service. A new protocol between the VO and HO is defined for device authentication and to exchange key used to protect the traffic between the VO and the device.

The VO is responsible for applying the security mechanism described in the following section, including the generation of the key used to protect the traffic.

The HO is responsible for authenticating and authorizing a device to access the roaming service.

An overview of the security architecture is depicted in Figure 6: -

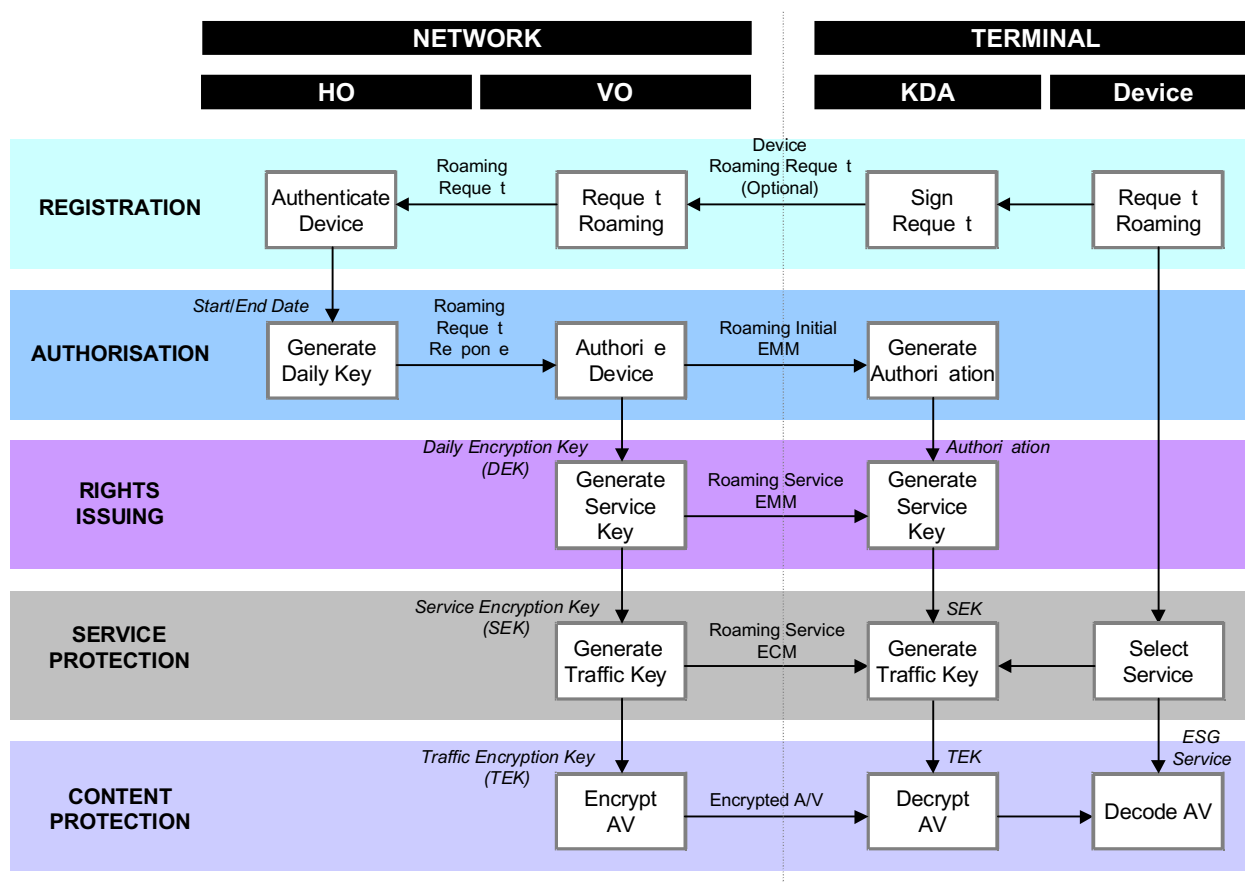


Figure 6: Overview of Roaming Security Architecture

7.2.1 Registration

Service negotiation is carried out either via web page or a phone call. A service package is selected by the subscriber and registration initiated.

Device registration shall take advantage of the interaction channel, when available. The Device_Roaming_Request message is used by the Device to request roaming service from the VO. The Device_Roaming_Request message includes a device signature, which is used by the HO to authenticate the device.

The Device_Roaming_Request message is passed to the HO in a Roaming_Request message from the VO. The VO signs the Roaming_Request message to enable authenticated communication. The HO checks that the Device belongs to a valid subscriber and that the subscriber can be authorized for roaming service.

7.2.2 Authorisation

The HO generate a device authorisation and a series of Daily Encryption Key (DEK) for the requested roaming period and send them along with the DEK Key Material to the VO in the Roaming_Request_Response message.

The VO send the device authorisation and the certificate of the VO in the Roaming_Initial_EMM message to the device. This message includes a HO signature of the VO certificate ID and roaming date range, provided by the HO in the Roaming_Request_Response message. The VO certificate exchange is used to enable authenticated communication between the VO and the Device and ensure signalling protection against unauthorised modification of the messaging.

The Roaming_Initial_EMM message authorises the device for roaming from the VO for a given period of time.

7.2.3 Right Issuing

The VO is responsible for generating a Service Encryption Key (SEK) for each roaming service requiring service protection on a given day. The SEK is sent to the device in the Roaming_Service_EMM message.

The key transfer is confidentiality protected by encrypting the SEK with the DEK for the specific day. The corresponding DEK Key Material is sent with the encrypted SEK within the Roaming_Service_EMM message. The VO signs this message with its public key to ensure data integrity and authentication of the received message by the device.

The Roaming_Service_EMM provides the device with the rights needed to access each authorised roaming service.

7.2.4 Service Protection

The VO generates Traffic Encryption Key (TEK) for each roaming service, which are applied directly to the ISMACryp scrambler to protect the content. The TEKs are sent to the device in Roaming_Service_ECM message. The VO creates a Roaming_Service_ECM message stream for each roaming service.

The VO operator ensures confidentiality of the TEK by encrypting the content of the Roaming_Service_ECM message with the SEK for the roaming service with which the message stream is associated.

The Roaming_Service_ECM includes an unencrypted roaming_service_id field to enable the device to identify the SEK needed to decrypt the message.

The Roaming_Service_ECM messages are cycled to support random access of a roaming service. The message stream supports re-keying using the ISMACryp specified Key Indicator mechanism.

7.2.5 Content Protection

The VO encrypts the content with the TEK. Re-keying of the TEK by the VO provides protection against key-distribution attacks.

Content Access Unit (AU) are encrypted with the TEK using ISMACryp 1.0 AES-128 Counter Mode. The details of Content Protection scheme can be found in reference [7].

7.3 Key Management and Distribution

7.3.1 Daily Encryption Key

The HO shall generate a set of DEKs for each device requiring roaming. There shall be a DEK for each day that the device is authorised for roaming.

The DEK shall be generated by a KMS-specific one-way hash function:

$$\text{DEK} = \text{HASH}(\text{roaming_random_data} \parallel \text{roaming_date}, \text{device_id})$$

Where, roaming_random_data and roaming_date are provided to the VO with each DEK in the Roaming_Request_Response message and transmitted to the device in the Roaming_Service_EMM message.

For security reason, it is recommended that the hash function is implemented in the SIM rather than the KDA. It is assumed that all SIM cards have the capability to perform a one-way hash function.

A DEK shall be identified by a roaming_date in the Roaming_Service_EMM message. The roaming_date identifies the day during which the DEK is valid.

7.3.2 Service Encryption Key

The VO shall generate SEK for roaming service. One or more roaming service may share the same SEK.

The symmetric encryption scheme AES ECB shall be used to securely transmit the SEK to a device using the DEK provided to the VO in the Roaming_Request_Response message: -

$$\text{encrypted_SEK} = \text{AES-ECB.ENCRYPT}(\text{SEK}, \text{DEK}).$$

The VO using RSA-PSS-Default signs the Roaming_Service_EMM message used to transport the encrypted_SEK to the device:

<http://www.rsa-secrity.com/ralab/pkc/chema/pkc-1#rsa-pss-default>

The hash algorithm to be used (before applying RSA with padding) shall be SHA-1.

A SEK shall be identified by a roaming_service_id in the Roaming_Service_EMM and the Roaming_Service_ECM message. The VO shall change the roaming_service_id each time there is a SEK key change.

7.3.3 Traffic Encryption Key

The VO shall generate TEK for roaming service. Each roaming service shall be encrypted by a sequence of time-varying TEK.

The symmetric encryption scheme AES CBC mode shall be used to securely transmit the TEK to recipient device using the SEK generated by the VO.

The TEK shall be identified by a Key Indicator in the Roaming_Service_ECM message. The Key Indicator shall be used to synchronize the TEK with the encrypted A/V.

7.4 Key Generation and Validation at the Device

The Roaming_Initial_EMM is signed by the HO and authenticated by the KDA. The KDA uses the VO certificate received in this message to validate the Roaming_Service_EMM message.

The KDA securely generates the DEK from the Key Material transmitted in the Roaming_Service_EMM message. The KDA uses a KMS specific one-way hash function to generate the DEK.

The KDA securely generates the SEK from the Roaming_Service_EMM message using the DEK to decrypt the encrypted_SEK.

The KDA securely generates the TEK from the Roaming_Service_ECM message using the appropriate SEK to decrypt the message. The required SEK is identified by the roaming_service_id within the Roaming_Service_ECM message.

The KDA sends the TEK to the Device Decrambler.

7.5 Roaming Message

7.5.1 Device Roaming Request

The Device Roaming Request message is used to request a service from the VO. This message is optional and is only used where the device has interaction channel capabilities. The purpose of the request is for the VO to prove to the HO that a device has indeed requested service. A signature is appended to a request, verifying that the real device is involved.

7.5.2 Roaming Request

This request is used for the VO to ask the HO to authenticate and authorize the device to access roaming service for the requested number of day.

Syntax	No. of bit	Identifier
dvb_h_roaming_vo_to_ho() {		
device_id	64	b lbf
ho_id	32	uim bf
vo_id	32	
number_of_day_requested	8	
request_type	8	
if request_type = 1 {	32	uim bf
request_len	16	b lbf
device_roaming_request	var	b lbf
}		
vo_certificate_id	ee x509	
vo_signature	1024	
}		

Semantic :-

device_id: ID of the device requesting the service

ho_id: ID of the home operator service provider

vo_id: ID of the visiting service provider requesting the service for the device

number_of_day_requested: Number of day for which roaming service are requested.

request_type: Is this a voice request (0) or a 2-way request (1).

request_len: length of the appended request structure.

request_type: appended request structure.

vo_certificate_id: ID of the VO certificate.

vo_signature: VO signature on this request over the entire structure.

Note: -

RSA-PSS-Default: <http://www.rsa-security.com/ralab/pkc/chema/pkc-1#rsa-pss-default>

The hash algorithm to be used (before applying RSA with padding) is SHA-1.

7.5.3 Roaming Request Response

The Roaming Request Response is used to transfer the device authorization and DEK from the HO to the VO.

Syntax	No. of bit	Identifier
dvb_h_roaming_ho_to_vo() {		
device_id	64	B lbf
ho_id	32	uim bf
vo_id	32	
number_of_day	8	
for (n=0; n < number_of_day ; n++) {		
roaming_date	16	uim bf
roaming_random_data	112	B lbf
daily_encryption_key	128	B lbf

Syntax	No. of bit	Identifier
}		
ho_ignature_of_vo_certificate_and_date_range	128	
ho_certificate_id	ee x509	
ho_ignature	1024	
}		

Semantic : -

device_id: ID of the device requesting the service

ho_id: ID of the home operator service provider

vo_id: ID of the visiting service provider requesting the service for the device

number_of_day : Number of day for which key are being given.

roaming_date: The date on which the key indicated in 'daily_encryption_key' is valid. The date format is the lower 16 bit of the MJD.

roaming_random_data: Random bit chosen by the HO to be used in the generation of the daily_encryption_key.

daily_encryption_key: A key to be used for signing/encrypting EMM. This key is KMS-specific and is based on using the roaming_date, roaming_random_data and device_id as input.

ho_ignature_of_vo_certificate_and_date_range: The HO KMS-specific signature of the public_id of the VO concatenated with the time and date range of validity. This will be communicated to the KDA/SIM to tell it that access is being granted. This can be unique to a specific device.

ho_certificate_id: ID of the HO certificate used for producing ho_ignature. Certificate distribution is out of the scope of this proposal.

ho_ignature: RSA signature on this request over the entire structure.

7.5.4 Roaming_Initial_EMM

This message is used for the HO to authorize a device for roaming from a VO for a given number of day. A specially designated CAS_ID is used to show that this is a roaming EMM.

Syntax	No. of bit	Identifier
dvb_h_roaming_initial_emm() {		
length	14	uim bf
type	2	uim bf
device_id	64	b lbf
vo_cert_id	32	a cii
vo_certificate	ee x509	b lbf
start_date	16	uim bf
end_date	16	uim bf
ho_ignature_of_vo_certificate_and_date_range	128	uim bf
}		

Semantic

length: The length of the dvb_h_roaming_initial_emm structure (including this field)

type: A value of 0 signals a Roaming_Initial_EMM. A value of 1 signals a Roaming_Service_EMM (see below). Other values are reserved. EMM signalled with other values MUST be ignored.

device_id: This field identifies the device for which this EMM is addressed.

vo_cert_id: certificate id of the VO initiating this EMM.

vo_certificate: TBD either a full X509 certificate or alternatively just the public key of the VO.

start_date: start date that the device can accept key from this VO (expressed as a lower 16 bit of MJD).

end_date: end date for accepting key from this VO (expressed as a lower 16 bit of MJD).

ho_signature_of_vo_certificate_and_date_range: The HO KMS-specific signature of the public_id of the VO concatenated with the time and date range of validity. This can be unique to a specific device.

7.5.5 Roaming_Service_EMM

This message is used to entitle the device to access roaming service and deliver the SEK. A specially designated CAS_ID is used to show that this is a roaming EMM.

Syntax	No. of bit	Identifier
dvb_h_roaming_emm() {		
length	14	uim bf
type	2	uim bf
device_id	64	b lbf
CA_system_id	16	uim bf
roaming_date	16	a cii
roaming_random_data	112	b lbf
number_of_service	8	uim bf
for (n=0; n < number_of_service ; n++) {		
roaming_service_id	32	uim bf
encrypted_service_encryption_key	128	b lbf
}		
vo_certificate_id		
vo_random_signature		
}		

Semantic : -

length: The length of the dvb_h_roaming_emm structure (including this field)

type: A value of 1 signals a Roaming_Service_EMM. A value of 0 signals a Roaming_Initial_EMM (see above). Other values are reserved. EMM signalled with other value MUST be ignored.

device_id: This field identifies the device for which this EMM is addressed.

CA_system_id: This 16-bit field identifies the KMS. Allocation of the value of this field are found in ETR 162 [6].

roaming_date: The date the key indicated in encrypted_service_encryption_key is valid. (Expressed as a lower 16 bit of MJD)

roaming_random_data: A random 112-bit number.

number_of_service : Number of service contained in this EMM.

roaming_service_id: The service ID for which the key that follows is valid.

encrypted_service_encryption_key: The service encryption key encrypted using the Daily Encryption Key provided to the VO in the dvb_h_roaming_vo_to_ho message using AES ECB mode.

vo_certificate_id: Certificate for producing Signature.

vo_emm_signature: EMM Signature.

7.5.6 Roaming_Service_ECM

The Roaming_Service_ECM message contains the time at which the ECM was built, which acts both as a source of time for the smartcard and as the date at which the ECM is valid. It also contains the identifier of the service it gives access to, and a pair of Key Indicator/TEK couple. The ECM structure contained within the encrypted_section of the message is encrypted with the Service Encryption Key using AES 128 in CBC mode.

Syntax	No. of bit	Identifier
dvb_h_roaming_ecm() {		
length	14	uim bf
type	2	uim bf
roaming_service_id	32	uim bf
{		
time	32	uim bf
roaming_service_id	32	uim bf
key_indicator_1	32	uim bf
traffic_encryption_key_1	128	b lbf
key_indicator_2	32	uim bf
traffic_encryption_key_2	128	b lbf
} encrypted_section		
}		

Semantic : -

length: The length of the dvb_h_roaming_ecm structure (including this field).

type: A value of 0 signals a Roaming_Service_ECM, other values are reserved. ECM signalled with a type other than 0 MUST be ignored.

time: the time at which this ECM was generated, in seconds since January 1, 1970, UTC, and the date of validity of the ECM.

roaming_service_id: The service ID for which the key that follows is valid.

key_indicator_n: The identifier of traffic encryption key n

traffic_encryption_key_n: Traffic encryption key n

8 Annex A (Informative): Adaptation of DVB Simulcrypt interface to the DVB-H Environment

This chapter describes how the DVB Simulcrypt interface may be adapted to the DVB-H environment, according to the DVB-CBMS specification.

8.1 Reference DVB-Headend Architecture

The following figure describes DVB-Headend reference architecture as it is done in reference [1].

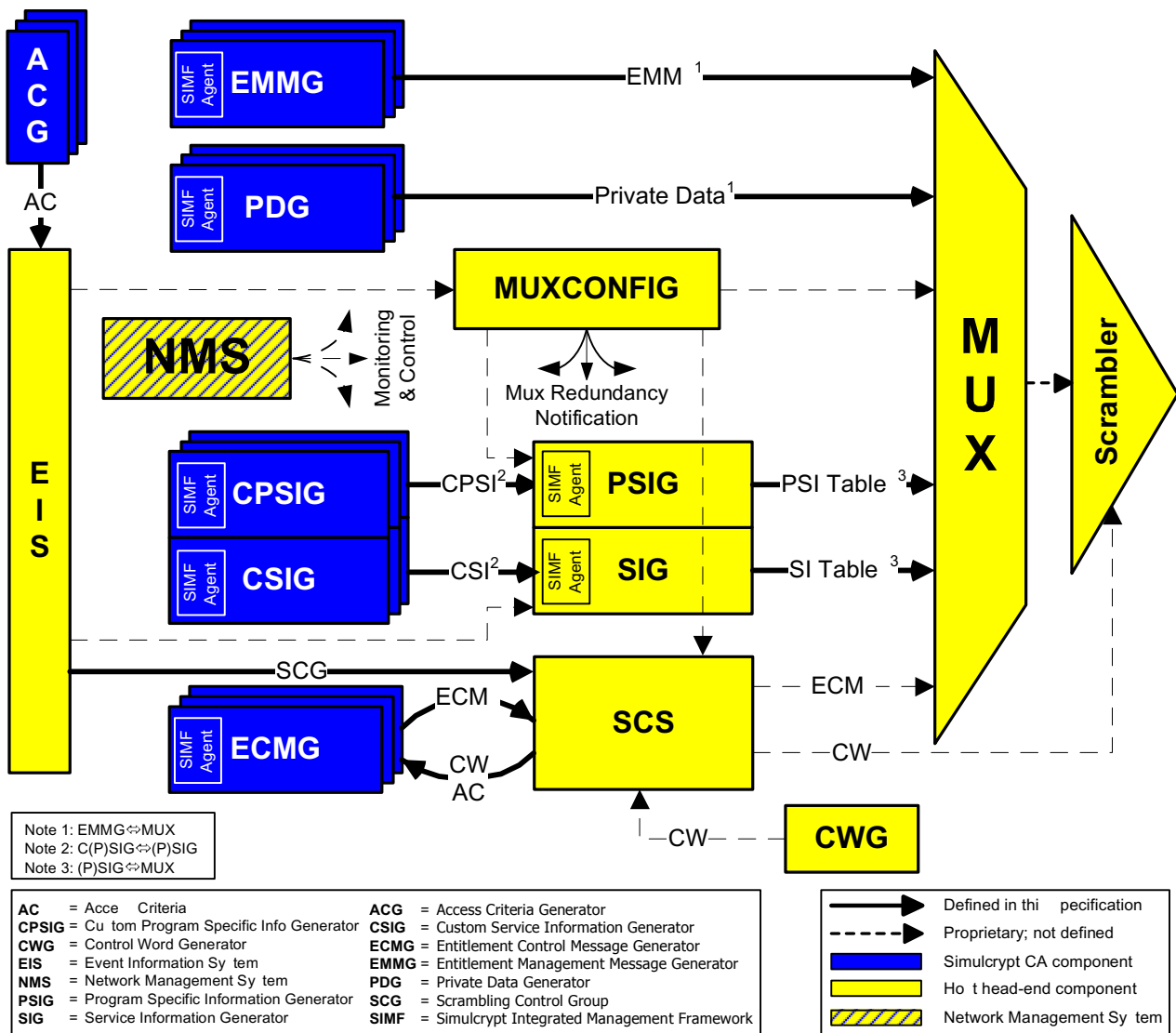


Figure 7: Reference DVB Headend Architecture

Note: in this specification TEK is used to mean CW.

8.2 DVB-H Headend Architecture and Interface

The DVB-H Headend architecture is shown in Figure 8: -

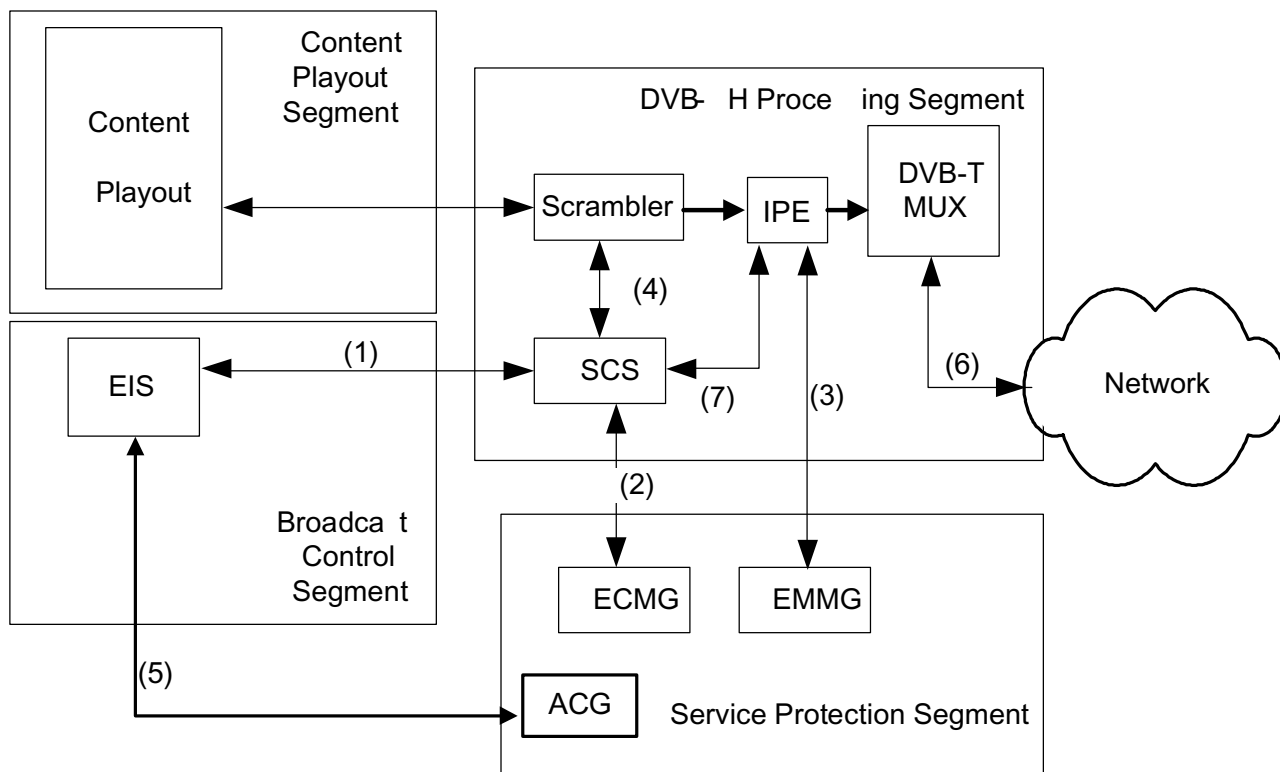


Figure 8: DVB-H Headend Architecture

The reference architecture can be mapped to DVB-H Headend architecture as follows:

1. Interface EIS \leftrightarrow SCS (see #1 on Fig 8) should be implemented according to section #10 EIS \leftrightarrow SCS interface from [1]. The OpenCAS interface implementation is also acceptable.
2. Interface ECMG \leftrightarrow SCS (see #2 on Fig 8) should be implemented according to section #5 ECMG \leftrightarrow SCS interface from [1].
3. Interface EMMG \leftrightarrow IPE (see #3 on Fig 8) should be implemented according to section #6 EMMG \leftrightarrow MUX interface from [1].
4. Interface SCS \leftrightarrow ISMACryp Scrambler is not defined in [1] and can be proprietary per ISMACryp Scrambler provider.
5. Interface EIS \leftrightarrow ACG Interface EMMG \leftrightarrow MUX (see #5 on Fig 8) should be implemented according to section #10 EIS \leftrightarrow ACG interface from [1].
6. DVB-T transport stream
7. Interface SCS \leftrightarrow IPE (see #7 on Fig 8).

8.3 DVB-H Headend Architecture for Roaming Support

Figure 9 depicts the DVB-H Headend architecture that includes roaming support.

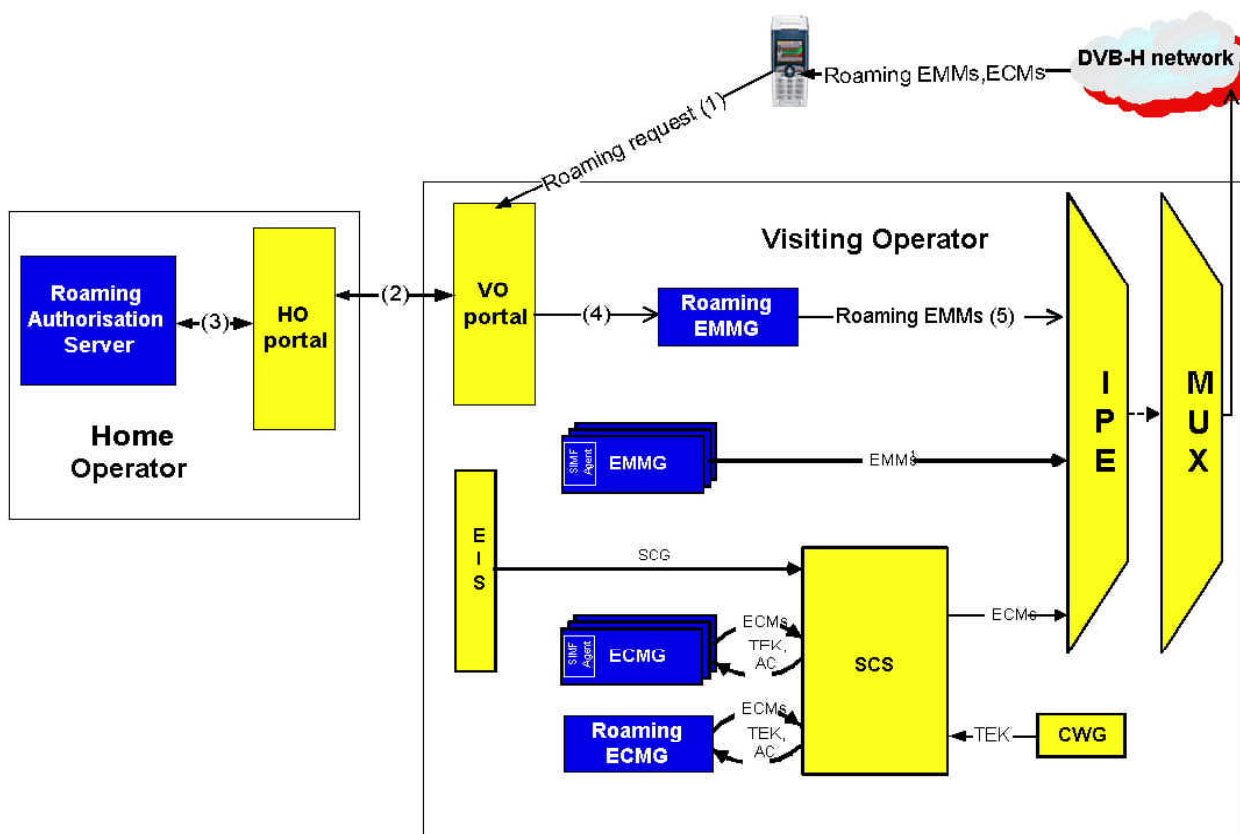


Figure 9: DVB-H Headend Architecture including roaming support

8.3.1 Roaming ECM

The special Roaming ECMG should be applied to generate roaming ECM. This ECMG should have dedicated Roaming CAS ID for roaming.

The AC for roaming ECM generation should contain roaming_service_id for each ECMG stream.

In the ecmg channel_setup message the roaming ECMG should be configured to receive current and next TEK.

8.3.2 Roaming EMM

The protocol (1) (see Fig 9) is used to transfer Device Roaming Request from device to VO as defined in [3]. The protocol can be standardized as XML over HTTP.

The protocol (2) (see Fig 9) is used to transfer Roaming Request and Roaming Request Response between VO and HO. The protocol can be standardized as XML over HTTP. The binary content of the message is defined in section 7.5.

The protocol (3) (see Fig 9) is used for communication between HO and the Roaming Authorisation Server.

The protocol (4) (see Fig 9) is used to transfer information for generation Roaming_Initial_EMM and Roaming_Service_EMM from VO portal to visiting EMMG. The protocol can be standardized as XML over HTTP - the binary content of the message is defined in this specification.

The protocol (5) is defined in reference [1] Section #5 EMMG ↔ MUX protocol

9 Annex B (Informative): Using OMA BCAST as a Key Management System

This chapter describes how OMA BCAST may be used as a Key Management System to control access to content broadcast according to the DVB-CBMS specification.

9.1 Overview

OMA BCAST is a fully standardised system allowing operator to control access and usage of broadcast content on mobile device. The full specification are currently being drafted within OMA.

The abstraction layer described in chapter 5.2, and key hierarchy associated to it is unchanged. The role of OMA BCAST based system is to manage right by delivering Service Encryption Key to entitled device. The Service Encryption Key allow the entitled device to decrypt ECM for that service and in turn the content.

The OMA BCAST system therefore fits in the Open Framework as one possible Key Management System and can be used as such.

9.2 Registration

To be recognised as a valid KMS, OMA BCAST system need to register a single unique CAS_ID value, valid for all compliant system. This CAS_ID will then be used to filter EMM and ECM.

9.3 EMM

OMA BCAST may be used to manage right through the distribution of Right Object. In case RO need to be distributed using the broadcast feed, they may be carried as EMM. This form of distribution is in no way mandatory and Right Object may be carried to the receiver in any way deemed appropriate, in particular through a cellular network.

The Right Object giving access to a service/program contains the Service Encryption Key/Program Encryption Key for that service/program. In other words, the Right Object does not, in fact, give access to the content itself, but rather to the Key Stream Message (KSM) containing the key to decrypt the content: in OMA parlance, the actual RO gives access to the KSM.

An RO is distributed as an EMM in a UDP packet as part of an EMM stream signalled with the afore-mentioned CAS_ID. It is the responsibility of the OMA-BCAST KDA to setup the appropriate EMM filter corresponding to the unique device ID and possibly multiple group ID assigned to the device and to further apply the group Access Mask found in the message proper in case of group addressing.

9.4 ECM

OMA BCAST defines a fully standardised Key Stream layer where Key Stream Messages (KSM) take the role of ECM. The Key Stream Messages are carried in UDP packets as ECM and distinguished from other system ECM through the use of the registered OMA-BCAST CAS_ID.

Bibliography

The following material, though not specifically referenced in the body of the present document (or not publicly available), give supporting information.

- ETSI ETR 289: "Digital Video Broadcasting (DVB); Support for use of scrambling and Conditional Access (CA) within digital broadcasting system".
- Implementation guideline for use of telecommunication interface in the Digital Broadcasting system (DVB Project Office).

10 History

Document history		
Issue 1A	18/01/2005	Initial draft